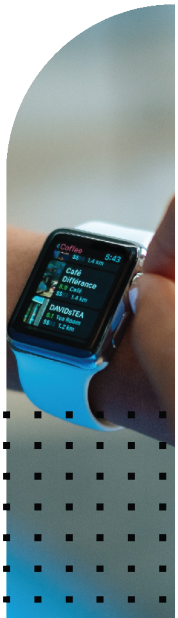
# Release Notes

## FortiOS 7.0.10



**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

February 23, 2023
FortiOS 7.0.10 Release Notes
01-7010-880549-20230223

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2023-02-23 | Initial release. |
| 2023-02-27 | Updated Known issues on page 24. |

# Introduction and supported models

This guide provides release information for FortiOS 7.0.10 build 0450.

For FortiOS documentation, see the Fortinet Document Library.

## Supported models

FortiOS 7.0.10 supports the following models.

| | |
|---|---|
| **FortiGate** | FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1 |
| **FortiWiFi** | FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE |
| **FortiGate Rugged** | FGR-60F, FGR-60F-3G4G |
| **FortiGate VM** | FG-ARM64-AWS, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN |
| **Pay-as-you-go images** | FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN |

### Special branch supported models

The following models are released on a special branch of FortiOS 7.0.10. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0450.

| | |
|---|---|
| **FG-400F** | is released on build 4913. |
| **FG-401F** | is released on build 4913. |
| **FG-600F** | is released on build 4913. |

| | |
|---|---|
| **FG-601F** | is released on build 4913. |
| **FG-80F-DSL** | is released on build 4921. |
| **FG-1000F** | is released on build 6521. |
| **FG-1001F** | is released on build 6521. |
| **FG-3000F** | is released on build 4913. |
| **FG-3001F** | is released on build 4913. |
| **FG-3200F** | is released on build 6527. |
| **FG-3201F** | is released on build 6527. |
| **FG-3700F** | is released on build 6527. |
| **FG-3701F** | is released on build 6527. |
| **FG-4800F** | is released on build 6527. |
| **FG-4801F** | is released on build 6527. |
| **FGR-70F** | is released on build 6524. |
| **FGR-70F-3G4G** | is released on build 6524. |

# Special notices



## Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

## GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

## ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

# Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1:

- Facebook
- Gmail
- Office 365
- YouTube

# RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1.

# CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

# FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

## Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.0.10 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For more information, refer to the Hyperscale Firewall Release Notes.

# Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

**To view supported upgrade path information:**

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

## Fortinet Security Fabric upgrade

FortiOS 7.0.10 greatly increases the interoperability between other Fortinet products. This includes:

| | |
|---|---|
| **FortiAnalyzer** | • 7.0.5 |
| **FortiManager** | • 7.0.5 |
| **FortiExtender** | • 4.0.0 and later. For compatibility with latest features, use latest 7.0 version. |
| **FortiSwitch OS (FortiLink support)** | • 6.4.6 build 0470 or later |
| **FortiAP**<br>**FortiAP-S**<br>**FortiAP-U**<br>**FortiAP-W2** | • See Strong cryptographic cipher requirements for FortiAP on page 13 |
| **FortiClient* EMS** | • 7.0.0 build 0042 or later |
| **FortiClient* Microsoft Windows** | • 7.0.0 build 0029 or later |
| **FortiClient* Mac OS X** | • 7.0.0 build 0022 or later |
| **FortiClient* Linux** | • 7.0.0 build 0018 or later |
| **FortiClient* iOS** | • 6.4.6 build 0507 or later |
| **FortiClient* Android** | • 6.4.6 build 0539 or later |
| **FortiSandbox** | • 2.3.3 and later |

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.0.0, use FortiClient 7.0.0.

Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI/FortiNDR
19. FortiTester
20. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.10. When Security Fabric is enabled in FortiOS 7.0.10, all FortiGate devices must be running FortiOS 7.0.10.

# Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings

- admin user account
- session helpers
- system access profiles

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

## IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

## HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

## Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

## How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

## L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

**To make L2TP over IPsec work after upgrading:**

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

   ```
   config vpn l2tp
       set eip 210.0.0.254
       set sip 210.0.0.1
       set status enable
       set usrgrp "L2tpusergroup"
   end
   ```

   Add a static route after upgrading:

   ```
   config router static
       edit 1
           set dst 210.0.0.0 255.255.255.0
           set device "l2t.root"
       next
   end
   ```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

# Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

## Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

During the upgrade process after the FortiGate reboots, the following message is displayed:

```
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
```

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -
61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -
61)
```

## Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.

- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

## Example configurations

`vip46` object:

| Old configuration | New configuration |
|---|---|
| `config firewall vip46`<br>`edit "test-vip46-1"`<br>`set extip 10.1.100.155`<br>`set mappedip 2000:172:16:200::55`<br>`next`<br>`end` | `config firewall vip`<br>`edit "test-vip46-1"`<br>`set extip 10.1.100.150`<br>`set nat44 disable`<br>**`set nat46 enable`**<br>`set extintf "port24"`<br>**`set ipv6-mappedip 2000:172:16:200::55`**<br>`next`<br>`end` |

`ippool6` object:

| Old configuration | New configuration |
|---|---|
| `config firewall ippool6`<br>`edit "test-ippool6-1"`<br>`set startip 2000:172:16:201::155`<br>`set endip 2000:172:16:201::155`<br>`next`<br>`end` | `config firewall ippool6`<br>`edit "test-ippool6-1"`<br>`set startip 2000:172:16:201::155`<br>`set endip 2000:172:16:201::155`<br>**`set nat46 enable`**<br>`next`<br>`end` |

NAT46 policy:

| Old configuration | New configuration |
|---|---|
| `config firewall policy46`<br>`edit 1`<br>`set srcintf "port24"`<br>`set dstintf "port17"`<br>`set srcaddr "all"`<br>`set dstaddr "test-vip46-1"`<br>`set action accept`<br>`set schedule "always"`<br>`set service "ALL"`<br>`set logtraffic enable`<br>`set ippool enable` | `config firewall policy`<br>`edit 2`<br>`set srcintf "port24"`<br>`set dstintf "port17"`<br>`set action accept`<br>**`set nat46 enable`**<br>`set srcaddr "all"`<br>`set dstaddr "test-vip46-1"`<br>`set srcaddr6 "all"`<br>`set dstaddr6 "all"`<br>`set schedule "always"` |

| Old configuration | New configuration |
|---|---|
| `set poolname "test-ippool6-1"`<br>`next`<br>`end` | `set service "ALL"`<br>`set logtraffic all`<br>`set ippool enable`<br>`set poolname6 "test-ippool6-1"`<br>`next`<br>`end` |

`vip64` object

| Old configuration | New configuration |
|---|---|
| `config firewall vip64`<br>`edit "test-vip64-1"`<br>`set extip 2000:10:1:100::155`<br>`set mappedip 172.16.200.155`<br>`next`<br>`end` | `config firewall vip6`<br>`edit "test-vip64-1"`<br>`set extip 2000:10:1:100::155`<br>`set nat66 disable`<br>**`set nat64 enable`**<br>**`set ipv4-mappedip 172.16.200.155`**<br>`next`<br>`end` |

`ippool` object

| Old configuration | New configuration |
|---|---|
| `config firewall ippool`<br>`edit "test-ippool4-1"`<br>`set startip 172.16.201.155`<br>`set endip 172.16.201.155`<br>`next`<br>`end` | `config firewall ippool`<br>`edit "test-ippool4-1"`<br>`set startip 172.16.201.155`<br>`set endip 172.16.201.155`<br>**`set nat64 enable`**<br>`next`<br>`end` |

NAT64 policy:

| Old configuration | New configuration |
|---|---|
| `config firewall policy64`<br>`edit 1`<br>`set srcintf "wan2"`<br>`set dstintf "wan1"`<br>`set srcaddr "all"`<br>`set dstaddr "test-vip64-1"`<br>`set action accept`<br>`set schedule "always"`<br>`set service "ALL"`<br>`set ippool enable`<br>`set poolname "test-ippool4-1"`<br>`next`<br>`end` | `config firewall policy`<br>`edit 1`<br>`set srcintf "port24"`<br>`set dstintf "port17"`<br>`set action accept`<br>**`set nat64 enable`**<br>`set srcaddr "all"`<br>`set dstaddr "all"`<br>`set srcaddr6 "all"`<br>`set dstaddr6 "test-vip64-1"`<br>`set schedule "always"`<br>`set service "ALL"`<br>`set logtraffic all` |

| Old configuration | New configuration |
| --- | --- |
| | set ippool enable<br>set poolname "test-ippool4-1"<br>next<br>end |

# ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`.
- To display the `srcintf` as *any* in the GUI, *System* > *Feature Visibility* should have *Multiple Interface Policies* enabled.
- All full ZTNA firewall policies will be automatically removed.

# Default DNS server update

If both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

# Product integration and support

The following table lists FortiOS 7.0.10 product integration and support information:

| | |
|---|---|
| **Web browsers** | • Microsoft Edge 94<br>• Mozilla Firefox version 105<br>• Google Chrome version 107<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **Explicit web proxy browser** | • Microsoft Edge 44<br>• Mozilla Firefox version 74<br>• Google Chrome version 80<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiController** | • 5.2.5 and later<br>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C |
| **Fortinet Single Sign-On (FSSO)** | • 5.0 build 0309 and later (needed for FSSO agent support OU in group filters)<br>  • Windows Server 2022 Standard<br>  • Windows Server 2019 Standard<br>  • Windows Server 2019 Datacenter<br>  • Windows Server 2019 Core<br>  • Windows Server 2016 Datacenter<br>  • Windows Server 2016 Standard<br>  • Windows Server 2016 Core<br>  • Windows Server 2012 Standard<br>  • Windows Server 2012 R2 Standard<br>  • Windows Server 2012 Core<br>  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)<br>  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)<br>  • Windows Server 2008 Core (requires Microsoft SHA2 support package)<br>  • Novell eDirectory 8.8 |
| **AV Engine** | • 6.00282 |
| **IPS Engine** | • 7.00157 |

## Virtualization environments

The following table lists hypervisors and recommended versions.

| Hypervisor | Recommended versions |
|---|---|
| **Citrix Hypervisor** | • 8.1 Express Edition, Dec 17, 2019 |
| **Linux KVM** | • Ubuntu 18.0.4 LTS<br>• Red Hat Enterprise Linux release 8.4<br>• SUSE Linux Enterprise Server 12 SP3 release 12.3 |
| **Microsoft Windows Server** | • 2012R2 with Hyper-V role |
| **Windows Hyper-V Server** | • 2019 |
| **Open source XenServer** | • Version 3.4.3<br>• Version 4.1 and later |
| **VMware ESX** | • Versions 4.0 and 4.1 |
| **VMware ESXi** | • Versions 6.5, 6.7, and 7.0. |

# Language support

The following table lists language support information.

**Language support**

| Language | GUI |
|---|---|
| English | ✓ |
| Chinese (Simplified) | ✓ |
| Chinese (Traditional) | ✓ |
| French | ✓ |
| Japanese | ✓ |
| Korean | ✓ |
| Portuguese (Brazil) | ✓ |
| Spanish | ✓ |

# SSL VPN support

## SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

**Supported operating systems and web browsers**

| Operating System | Web Browser |
|---|---|
| Microsoft Windows 7 SP1 (32-bit & 64-bit) | Mozilla Firefox version 105<br>Google Chrome version 107 |
| Microsoft Windows 10 (64-bit) | Microsoft Edge<br>Mozilla Firefox version 105<br>Google Chrome version 107 |
| Ubuntu 20.04 (64-bit) | Mozilla Firefox version 105<br>Google Chrome version 107 |
| macOS Monterey 12.4 | Apple Safari version 15<br>Mozilla Firefox version 105<br>Google Chrome version 107 |
| iOS | Apple Safari<br>Mozilla Firefox<br>Google Chrome |
| Android | Mozilla Firefox<br>Google Chrome |

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

# Resolved issues

The following issues have been fixed in version 7.0.10. To inquire about a particular bug, please contact Customer Service & Support.

## Firewall

| Bug ID | Description |
|---|---|
| 865661 | Standard and full ISDB sizes are not configurable on FG-101F. |

## Proxy

| Bug ID | Description |
|---|---|
| 818371 | WAD process crashes with some URIs. |
| 855882 | Increase in WAD process memory usage after upgrading. |
| 856235 | The WAD process memory usage gradually increases over a few days, causing the FortiGate to enter into conserve mode. |

## Routing

| Bug ID | Description |
|---|---|
| 847037 | When the policy route has a set gateway, the FortiGate is not following the policy route to forward traffic and sends unreasonable ARP requests. |

## Security Fabric

| Bug ID | Description |
|---|---|
| 839258 | Unable to add another FortiGate to the Security Fabric after updating to the latest patch. |

## SSL VPN

| Bug ID | Description |
|---|---|
| 746230 | SSL VPN web mode cannot display certain websites that are internal bookmarks. |
| 848067 | RDP over VPN SSL web mode stops work after upgrading. |

## System

| Bug ID | Description |
|---|---|
| 724085 | Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected. |
| 824543 | The `reply-to` option in the email server settings is no longer visible in a default server configuration on FortiOS 7.2.0. |
| 827240 | FortiGate in HA may freeze and reboot. Before the reboot, softIRQ may be seen as high. This leads to a kernel panic. |
| 847077 | `Can't find xitem. Drop the response.` error appears for DHCPOFFER packets in the DHCP relay debug. |
| 853794 | Issue with the `server_host_key_algorithm` compatibility when using SSH on SolarWinds. |
| 855573 | False alarm of the PSU2 occurs with only one installed. |
| 856202 | Random reboots and kernel panic on NP7 cluster when the FortiGate sends a TCP RST packet and IP options are missing in the header. |
| 859717 | The FortiGate is only offering the `ssh-ed25519` algorithm for an SSH connection. |

## Upgrade

| Bug ID | Description |
|---|---|
| 850691 | The `endpoint-control fctems` entry `0` is added after upgrading from 6.4 to 7.0.8 when the FortiGate does not have EMS server, which means the `endpoint-control fctems` feature was not enabled previously. This leads to a FortiManager installation failure. |

# Known issues

The following issues have been identified in version 7.0.10. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

## Anti Virus

| Bug ID | Description |
|---|---|
| 818092 | CDR archived files are deleted at random times and not retained. |
| 845960 | Flow mode opens port 8008 over the AV profile that does not have HTTP scan enabled. |

## Endpoint Control

| Bug ID | Description |
|---|---|
| 730767 | The new HA primary FortiGate cannot get EMS Cloud information when HA switches over.<br>**Workaround**: delete the EMS Cloud entry then add it back. |
| 834168 | FortiGates get deauthorized on EMS.<br>**Workaround**: manually authorize the affected FortiGates every ten minutes (approximately). |

## Explicit Proxy

| Bug ID | Description |
|---|---|
| 823319 | Authentication hard timeout is not respected for firewall users synchronized from WAD user. |
| 865135 | Multipart boundary parsing failed with CRLF before the end of boundary 1. |

# Firewall

| Bug ID | Description |
|---|---|
| 728734 | The VIP group hit count in the table (*Policy & Objects* > *Virtual IPs*) is not reflecting the correct sum of VIP members. |
| 794901 | Unable to create a `geography` type address object and get a `Can not be geography address when it is a member of addrgrp used by ipsec_tunnel!` error. |
| 840689 | Virtual server aborts connection when `ssl-max-version` is set to `tls-1.3`. |
| 847086 | Unable to add additional MAC address objects in an address group that already has 152 MAC address objects. |
| 852714 | Making a full HTTP session is sometimes bypassed if `ssl-hsts` is enabled for a `server-load-balance` VIP. |
| 854901 | Full cone NAT (`permit-any-host enable`) cause TCP session clash. |
| 860480 | FG-3000D cluster kernel panic occurs when upgrading from 7.0.5 to 7.0.6 and later. |
| 861990 | Increased CPU usage in softIRQ after upgrading from 7.0.5 to 7.0.6. |

# GUI

| Bug ID | Description |
|---|---|
| 440197 | On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly. |
| 677806 | On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status. |
| 685431 | On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies.<br>**Workaround**: use the CLI to configure policies. |
| 707589 | *System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed. |
| 708005 | When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator.<br>**Workaround**: use Chrome, Edge, or Safari as the browser. |

| Bug ID | Description |
|---|---|
| 722358 | When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode. |
| 755177 | When upgrading firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path. |
| 773258 | FortiAP icon cannot be moved once placed on the WiFi map. |
| 810225 | An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms. |
| 827893 | Security rating test result incorrectly shows *Failed* for FortiManager Cloud FortiCare support. |
| 833306 | Intermittent error, *Failed to retrieve FortiView data*, appears on real-time *FortiView Sources* and *FortiView Destination* monitor pages. |
| 843554 | The ALL service object is changed when a new object is created. |
| 845513 | On G-model profiles, changing the platform mode change from single 5G (dedicated scan enabled) to dual 5G is not taking effect. |
| 853352 | On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries. |

## HA

| Bug ID | Description |
|---|---|
| 662978 | Long lasting sessions are expired on HA secondary device with a 10G interface. |
| 777394 | Long-lasting sessions expire on the HA secondary in large session synchronization scenarios. |
| 810175 | `set admin-restrict-local` is not working for SSH. |
| 810286 | FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect. |
| 813207 | Virtual MAC address is sent inside GARP by the secondary unit after a reboot. |
| 818432 | When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures. |
| 830879 | Running `execute ha manage 0 <remote_admin>` fails and displays a `Permission denied, please try again.` error if the 169.254.0.0/16 local subnet is not in the trusted host list. |
| 835331 | Communication is disrupted when HA switching is performed in an environment where the VDOM is split to accommodate two IPoE lines. |
| 837888 | CLI deployment of a configuration to the secondary unit results in an unresponsive aggregate interface. |

| Bug ID | Description |
|---|---|
| 840305 | Static ARP entry is removed after reboot or HA failover. |
| 854445 | When adding or removing an HA monitor interface, the link failure value is not updated. |
| 860497 | Output of `diagnose sys ntp status` is misleading when run on a secondary cluster member. |
| 864226 | FG-2600F kernel panic occurs after a failover on both members of the cluster. |

## Hyperscale

| Bug ID | Description |
|---|---|
| 782674 | A few tasks are hung on issuing `stat verbose` on the secondary device. |
| 795853 | VDOM ID and IP addresses in the IPL table are incorrect after disabling EIF/EIM. |
| 807476 | After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with `unregister_vf`. If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled. |
| 811109 | FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG. |
| 836976 | Traffic impact on changing from log to hardware to log to host during runtime (with PPA enabled). |
| 838654 | Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic. |
| 839958 | `service-negate` does not work as expected in a hyperscale deny policy. |
| 842659 | `srcaddr-negate` and `dstaddr-negate` are not working properly for IPv6 traffic with FTS. |
| 843132 | After dynamically adding an ACL policy, the existing matched session is not cleared immediately. |
| 843197 | Output of `diagnose sys npu-session list/list-full` does not mention policy route information. |
| 843266 | Diagnose command should be available to show `hit_count/last_used` for policy route and NPU session on hyperscale VDOM. |
| 843305 | Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up. |
| 844421 | The `diagnose firewall ippool list` command does not show the correct output for overload type IP pools. |
| 846520 | NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover. |
| 877696 | Get KTRIE invalid node related error and kernel panic on standby after adding a second device into A-P mode HA cluster. |

## IPsec VPN

| Bug ID | Description |
|---|---|
| 761754 | IPsec aggregate static route is not marked inactive if the IPsec aggregate is down. |
| 810833 | IPsec static router gateway IP is set to the gateway of the tunnel interface when it is not specified. |
| 822651 | NP dropping packet in the incoming direction for SoC4 models. |

## Log & Report

| Bug ID | Description |
|---|---|
| 838357 | A deny policy with log traffic disabled is generating logs. |
| 850519 | *Log & Report* > *Forward Traffic* logs do not return matching results when filtered with *!<application name>*. |
| 850642 | Logs are not seen for traffic passing through the firewall. |
| 860264 | The miglogd process may send empty logs to other logging devices. |
| 873987 | High memory usage from miglogd processes even without traffic. |

## Proxy

| Bug ID | Description |
|---|---|
| 727629 | WAD encounters signal 11 crash. |
| 781613 | WAD crash occurs four times on FG-61F during stress testing. |
| 836101 | FortiGate is entering conserve mode due to a WAD memory leak. |
| 837724 | WAD crash occurs. |

## Routing

| Bug ID | Description |
|---|---|
| 618684 | When HA failover is performed to the other cluster member that is not able to reach the BFD neighbor, the BFD session is down as expected but the static route is present in the routing table. |

| Bug ID | Description |
|---|---|
| 708904 | `No IGMP-IF for ifindex` log points to multicast enabled interface. |
| 809321 | IS-IS LSP packets do not include the checksum and the authentication key (`[Checksum: [missing]], [Checksum Status: Not present] and authentication "hmac-md5 (54), message digest]`). |
| 848270 | Reply traffic from the DNS proxy (DNS database) is choosing the wrong interface. |
| 850862 | GUI does not allow an AS path to be to configured with multiple similar AS numbers. |
| 860075 | Traffic session is processed by a different SD-WAN rule and randomly times out. |
| 862165 | FortiGate does not add the route in the routing table when it changes for SD-WAN members. |
| 862418 | Application VWL crash occurs after FortiManager configuration push causes an SD-WAN related outage. |
| 865914 | When BSM carries multiple CRPs, PIM might use the incorrect prefix to update the mroute's RP information. |

## Security Fabric

| Bug ID | Description |
|---|---|
| 614691 | Slow GUI performance in large Fabric topology with over 50 downstream devices. |
| 794703 | Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results. |
| 798795 | API that registers appliances to the Fabric stopped working. |
| 801048 | During the FortiOS initialization process, there is a small chance that other services using UDP take the specific port that caused csfd initialization to fail. |
| 814674 | *Failed to retrieve upgrade progress* message appears when upgrading a FortiAP or FortiSwitch that is connected to a downstream FortiGate. |
| 825291 | FortiAnalyzer connection security rating fails for FortiAnalyzer Cloud. |
| 835765 | Automation stitch trigger is not working when the threshold based email alert is enabled in the configuration. |
| 870527 | FortiGate cannot display more than 500 VMs in a GCP dynamic address. |

## SSL VPN

| Bug ID | Description |
|---|---|
| 783167 | Unable to load GitLab through SSL VPN web portal. |

| Bug ID | Description |
|---|---|
| 803576 | Comments in front of `<html>` tag are not handled well in HTML file in SSL VPN web mode. |
| 810239 | Unable to view PDF files in SSL VPN web mode. |
| 819754 | Multiple DNS suffixes cannot be set for the SSL VPN portal. |
| 825810 | SSL VPN web mode is unable to access EMS server. |
| 828194 | SSL VPN stops passing traffic after some time. |
| 831069 | A blank page displayed after logging in to the back-end server in SSL VPN web mode. |
| 841788 | In policy-based NGFW mode, SSL VPN web mode access does not follow the firewall policy, accept for all destination addresses. |
| 850898 | OS checklist for the SSL VPN in FortiOS does not include macOS Ventura (13). |
| 852566 | User peer feature for one group to match to multiple user peers in the authentication rules is broken. |
| 854642 | Internal website with JavaScript is proxying some functions in SSL VPN web mode, which breaks them. |
| 863860 | RDP over SSL VPN web mode to a Windows Server changes the time zone to GMT. |
| 877896 | When accessing the VDOM's GUI in SSL VPN web mode, policies are only shown for a specific VDOM instead of all VDOMs. |

## Switch Controller

| Bug ID | Description |
|---|---|
| 813216 | FortiLink goes down when CAPWAP offloading is enabled or disabled. |

## System

| Bug ID | Description |
|---|---|
| 778794 | Incorrect values in NP7/hyperscale DoS policy anomaly logs. For packet rate-based meter log, the repeated numbers do not reflect the amount of dropped packets for a specific anomaly/attack; for the session counter meter log, the `pps` number is negative. |
| 784169 | When a virtual switch member port is set to be an alternate by STP, it should not reply with ARP; otherwise, the connected device will learn the MAC address from the alternate port and send subsequent packets to the alternate port. |
| 799487 | The debug zone uses over 400 MB of RAM. |
| 813162 | Kernel panic occurs after traffic goes through IPsec VPN tunnel and EMAC VLAN interface. |

| Bug ID | Description |
|---|---|
| 813607 | LACP interfaces are flapping after upgrading to 6.4.9. |
| 818452 | The `ifLastChange` SNMP OID only shows zeros. |
| 819667 | 1G copper SFP port is always up on FG-260xF. |
| 826490 | NP7 platforms may reboot unexpectedly when unable to handle kernel null pointer de-reference. |
| 827241 | Unable to resolve sp***.saas.ap***.com on a specific VDOM. |
| 833062 | FortiGate becomes unresponsive, and there are many WAD and forticron crashes. |
| 841932 | The GUI and API stopped working after loading many interfaces due to httpsd stuck in a D state (kernel I/O socket). |
| 845736 | After rebooting the FortiGate, the MTU value on the VXLAN interface was changed. |
| 845781 | Kernel panic and regular reboots occur on NP7 platforms, which are caused by FortiOS trying to offload a receiving ESP packet from the EMAC VLAN interface and convert to an IPv6 destination address with NAT46 NPU offloaded sessions. |
| 847314 | NP7 platforms may encounter random kernel crash after reboot or factory reset. |
| 847664 | Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot. |
| 849186 | Unexpected console error appears: `unregister_netdevice: waiting for pim6reg1 to become free. Usage count = 3`. |
| 850683 | Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF. |
| 850688 | FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs. |
| 853811 | Fortinet 10 GB transceiver LACP flapping when shut/no shut was performed on the interface from the switch side. |
| 870381 | Memory corruption or incorrect memory access when processing a bad WQE. |

# Upgrade

| Bug ID | Description |
|---|---|
| 854550 | After upgrading to 7.0.8, `replacemsg utm` parameters are not taken over and revert to the default. Affected replacement messages under `config system replacemsg utm`: `virus-html`, `virus-text`, `dlp-html`, `dlp-text`, and `appblk-html`. |

## User & Authentication

| Bug ID | Description |
|---|---|
| 765184 | RADIUS authentication failover between two servers for high availability does not work as expected. |
| 835859 | Incorrect source MAC address is used in LLDP TX packet when the interface has `https` in `allowaccess`. |
| 842517 | Adding a local user to a group containing many users causes a delay in GUI and CLI due to cmdbsvr (high CPU). |
| 851233 | FortiToken activation emails should include HTTPS links to documentation instead of HTTP. |
| 853793 | FG-81F 802.1X MAC authentication bypass (MAB) failed to authenticate Cisco AP. |

## VM

| Bug ID | Description |
|---|---|
| 740796 | IPv6 traffic triggers `<interface>: hw csum failure` message on CLI console. |
| 764392 | Incorrect VMDK file size in the OVF file for hw13 and hw15.<br>**Workaround**: manually correct the hw13 and hw15 OVF file's `ovf:size` value. |
| 856645 | Session is not crated over NSX imported object when traffic starts to flow. |
| 859165 | Unable to enable FIPS cipher mode on FG-VM-ARM64-AWS. |
| 860096 | CPU spike observed on all the cores in a GCP firewall VM. |
| 869359 | Azure auto-scale HA shows certificate error for secondary VM. |

## WAN Optimization

| Bug ID | Description |
|---|---|
| 728861 | HTTP/HTTPS traffic cannot go through when `wanopt` is set to manual mode and an external proxy is used.<br>**Workaround**: set `wanopt` to automatic mode, or `set transparent disable` in the `wanopt profile`. |

## Web Filter

| Bug ID | Description |
|---|---|
| 766126 | Block replacement page is not pushed automatically to replace the video content when using a video filter. |

## WiFi Controller

| Bug ID | Description |
|---|---|
| 858653 | Invalid wireless MAC OUI detected for a valid client on the network. |
| 865260 | Incorrect source IP in the self-originating traffic to RADIUS server. |
| 868022 | Wi-Fi clients on a RADIUS MAC MPSK SSID get prematurely de-authenticated by the secondary FortiGate in the HA cluster. |
| 882551 | FortiWiFi fails to act as the root mesh AP, and leaf AP does not come online. |

## ZTNA

| Bug ID | Description |
|---|---|
| 832508 | The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.0.8 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`.<br>After upgrading, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled.<br>**Workaround**: unset the `ztna-ems-tag` in the ZTNA firewall proxy policy, and then set it again. |
| 848222 | ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type.<br>An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found. |
| 865316 | Adding an EMS tag on the *Policy & Objects* > *Firewall Policy* edit page for a normal firewall policy forces NAT to be enabled. |

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

## Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com